

DOCKET FILE COPY ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In The Matter of

Implementation of the Telecommunications Act of 1996:

CC Docket No. 96-115

Telecommunications Carriers' Use of Customer Proprietary Network and Other Customer Information

Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended

CC Docket No. 96-149

**COMMENTS OF THE
TELECOMMUNICATIONS RESELLERS ASSOCIATION**

**TELECOMMUNICATIONS
RESELLERS ASSOCIATION**

Charles C. Hunter
Catherine M. Hannan
HUNTER COMMUNICATIONS LAW GROUP
1620 I Street, N.W.
Suite 701
Washington, D.C. 20006
(202) 293-2500

March 30, 1998

Its Attorneys

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY	ii
I. INTRODUCTION	2
II. RECOMMENDATIONS	9
III. CONCLUSION	15

SUMMARY

Sections 222(a) and 222(b) of the Communications Act contain the prohibitions long sought by resale carriers against abuse by network service providers of the competitively-sensitive data resale carriers are compelled to disclose in order to obtain network services. Section 222(a) imposes on all telecommunications carriers providing wholesale services the duty to protect the confidentiality of proprietary information of, and relating to, carriers reselling their services. Section 222(b) enhances this obligation by prohibiting the use by a telecommunications carrier in its own marketing efforts of proprietary information it receives or obtains from a resale carrier customer for purposes of providing network services to that resale carrier customer.

The customers of a resale carrier are its principal assets; indeed, the customers of a "switchless" resale carrier may well constitute all or virtually all of its assets. In order to obtain network services, a resale carrier must disclose to a generally far larger competitor comprehensive information regarding this critical asset. Indeed, unlike most competitors which jealously guard the identity of their customers, treating such information as trade secrets, a resale carrier must voluntarily disclose to its network service provider not only the names, addresses and service locations, but such key marketing data as contact points, for all its subscribers. Moreover, simply by virtue of its provision of network services to the resale carrier, a network service provider has direct access to such additional data as subscriber service requirements, traffic levels and usage patterns. Accordingly, a resale carrier's network service provider is in a position to inflict severe damage on the resale carrier's business if it appropriates and uses in its marketing efforts competitively-sensitive information received from the resale carrier.

The duties and obligations set forth in new Sections 222(a) and 222(b) of the Communications Act are remarkably clear and direct. Little, if any, "interpretation" of Sections 222(a) and 222(b) is thus required. If, however, Sections 222(a) and 222(b) are to have their intended effect, promulgation of implementing regulations is nonetheless essential.

The Commission's principal objective in adopting implementing regulations should be to ensure that a network service provider's retail sales and marketing personnel are not privy to, and do not have access to databases containing, information regarding the subscribers of the network service provider's resale carrier customers. Achieving this goal will require not only effective access restrictions, but incentives significant enough to motivate strict carrier compliance. Three steps are necessary to accomplish these twin ends. First, the Commission must require network service providers to "wall-off" resale carrier confidential data from retail sales and marketing personnel. Second, the Commission must hold network service providers to a strict liability standard for abuse of resale carrier confidential data by their employees or agents. And third, the Commission must rigorously enforce the mandates of Sections 222(a) and 222(b) by imposing heavy monetary sanctions for abuse of resale carrier confidential data.

The protections embodied in Sections 222(a) and 222(b) have been a long time coming and the product of much work by the resale carrier community. TRA urges the Commission in the strongest possible terms not to negate these critical safeguards by adopting inadequate implementing regulations. Access restrictions, accompanied by strict liability and serious penalties, are necessary to fulfill a clear Congressional mandate.

In The Matter of

CC Docket No. 96-115

Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended

CC Docket No. 96-149

The Telecommunications Resellers Association ("TRA"),¹ through undersigned counsel and pursuant to Section 1.415 of the Commission's Rules, 47 C.F.R. § 1.415, hereby submits its Comments in response to the *Further Notice of Proposed Rulemaking*, FCC 98-27, released by the Commission in the captioned docket on February 26, 1996 (the "*Notice*"). In this further phase of CC Docket No. 96-115, the Commission will address, among other things, the safeguards that are necessary to protect "the competitively-sensitive information of other carriers, including resellers

¹ A national trade association, TRA represents more than 650 entities engaged in, or providing products and services in support of, telecommunications resale. TRA was created, and carries a continuing mandate, to foster and promote telecommunications resale, to support the telecommunications resale industry and to protect and further the interests of entities engaged in the resale of telecommunications services.

and information service providers, from network providers that gain access to such information through their provision of wholesale services."² The Commission has further sought comment on what "further enforcement mechanisms . . . [it] should adopt to ensure carrier compliance with . . . [its] rules, or that may be necessary to encourage appropriate carrier discharge of their duty under section 222(a) to protect the confidentiality of customer information."³

I.

INTRODUCTION

While the resale carrier community has always taken the position that an underlying network service provider that obtains information regarding the subscribers of a resale carrier solely by virtue of its carrier/customer relationship with the resale carrier and utilizes such proprietary data to market its services to those subscribers not only violates its common carrier obligations, but is guilty of theft, there now exists an express statutory prohibition of such conduct. Sections 222(a) and 222(b) of the Communications Act of 1934 ("Communications Act"), as amended by Section 702 of the Telecommunications Act of 1996 ("Telecommunications Act"),⁴ contain the prohibitions long sought by resale carriers against abuse by network service providers of the competitively-sensitive data resale carriers are compelled to disclose in order to obtain network services.

Section 222(a) includes among the duty to "protect the confidentiality of proprietary information" imposed on all telecommunications carriers, the obligation to protect the confidentiality

² Notice, FCC 98-27 at ¶ 206.

³ Id. at ¶ 207.

⁴ 47 U.S.C. §§ 222(a), 222(b); Pub. L. No. 104-104, 110 Stat. 56, § 702 (1996).

of "the proprietary data of, and relating to, . . . telecommunications carriers reselling telecommunications services provided by a telecommunications carriers."⁵ Section 222(b) further prohibits "[a] telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service" from using such information "for its own marketing efforts," clearly limiting the use of such information to the provision of the telecommunications service provided to a resale carrier customer.⁶ In referencing Section 202(a) and 202(b), the Conference Report reiterates these obligations, confirming their straight forward directives.⁷

TRA fought hard to have these safeguards incorporated into the Telecommunications Act because the customers of a resale carrier are its principal assets; indeed, the customers of a "switchless" resale carrier may well constitute all or virtually all of its assets. In order to obtain network services, a resale carrier must disclose to a generally far larger competitor comprehensive information regarding this critical asset. Indeed, unlike most competitors which jealously guard the identity of their customers, treating such information as trade secrets, a resale carrier must voluntarily disclose to its network service provider not only the names, addresses and service locations, but such key marketing data as contact points, for all its subscribers. Moreover, simply by virtue of its provision of network services to the resale carrier, a network service provider has direct access to such additional data as subscriber service requirements, traffic levels and usage

⁵ 47 U.S.C. § 222(a).

⁶ 47 U.S.C. § 222(b).

⁷ Joint Statement of Managers, S. Conf. Rep. No. 104-230, 104th Cong., 2nd Sess., p. 205 (1996) ("Joint Explanatory Statement").

patterns. Thus, the network service provider can readily ascertain the precise telecommunications needs of each of the resale carrier's subscribers. And given that a network service provider knows the exact cost of service it is charging its resale carrier customer, it can generally determine the rates the resale carrier is charging its own subscribers. In other words, a resale carrier must provide its network service provider with all the information that that entity requires to raid the resale carrier's subscriber base.

Unfortunately, this is not a theoretical concern for resale carriers. For example, a large percentage of respondents to a 1994/95 TRA survey of its resale carrier members reported that their underlying carriers had solicited their subscribers using confidential information they had disclosed in order to obtain network services.⁸ Nearly 90 percent of those respondents using AT&T Corp. ("AT&T") as their network service provider reported such abuses. More than 50 percent of those respondents identifying Sprint Corp. ("Sprint") as their underlying carrier and roughly a third of those respondents identifying WorldCom, Inc. d/b/a LDDS/WorldCom ("WorldCom") as their network service provider registered similar complaints. Among AT&T resale carrier customers, over 60 percent characterized instances of such abuse of competitively-sensitive information as "very frequent" or "frequent," and nearly 90 percent identified the problem as "very serious" or "serious."

This survey data is obviously somewhat dated. Abuse of carrier confidential data is nowhere near as rampant in the domestic, interexchange market as it was in the early to mid 1990s, although instances of such abuse unfortunately continue to occur far more frequently than they

⁸ "Comments of the Telecommunications Resellers Association" in Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Therefor, CC Docket No. 79-252 filed on June 9, 1995 at Appx. 2, Chart 2.

should in a market characterized by the competitive provision of wholesale services. The survey data, however, retains its pertinence not only because abuse of carrier confidential data remains a sporadic problem in the interLATA toll market, but because resale carriers are aggressively moving into new markets, particularly the local, intraLATA toll and wireless markets. Abuse of carrier confidential data tends to increase proportionately with the market share of the network service provider. Incumbent local exchange carriers ("LECs") retain their monopoly or near monopoly position in the local market; the wireless market is only now being transformed from a duopoly into an oligopoly, with a relatively few providers holding the lion's share of the national wireless market. Hence, the Commission can expect abuse of carrier confidential data to rise as resale of these services increases.

As TRA has explained on a number of occasions in comments filed with the Commission, the relationship between resale carriers and their network service providers is an awkward one at best. While resale carrier customers generally contribute substantial wholesale revenues to their network service providers,⁹ they also compete fiercely with these same facilities-based carriers for retail dollars.¹⁰ And given that resale carriers generally target underserved and

⁹ Competition in the Interstate, Interexchange Marketplace, 6 FCC Rcd. 5880, ¶ 115 (1991), 6 FCC Rcd. 7255 (1991), 6 FCC Rcd. 7569 (1991), 7 FCC Rcd. 2677 (1992), *recon.* 8 FCC Rcd. 2659 (1993), 8 FCC Rcd. 3668 (1993), 8 FCC Rcd. 5046 (1993), *recon.* 10 FCC Rcd 4562 (1995) (resale carriers are "large customers").

¹⁰ As the Commission has recognized, a network service provider is being asked to "make available . . . [its] facilities and services to . . . a carrier[] that intend[s] to compete directly with . . . [it] for its customers and its control of . . . [its] market." Implementation of the Local Competition Provisions in the Telecommunications Act of 1996, 11 FCC Rcd. 15499, ¶ 55 (1996), *recon.* 11 FCC Rcd. 13042 (1996), *further recon.* 11 FCC Rcd. 19738 (1996), *further recon.*, FCC 97-295 (Oct. 2, 1997), *aff'd in part, vacated in part sub. nom. Iowa Utilities Board v. FCC*, 120 F.3d 753 (1997), *modified* 1997 U.S. App. LEXIS 28652 (8th Cir. Oct. 14, 1997),

neglected market niches,¹¹ the retail dollars for which resale carriers compete will likely be those generated by their network service providers' highest margin accounts. In other words, resale carriers will utilize the wholesale discounts they secure from their network service providers as a result of either statutory mandates or substantial volume and term commitments to market to customers these same underlying carriers had previously been able to take for granted.

As a result, network providers tend to be somewhat schizophrenic in their dealings with their resale carrier customers, treating them in some instances with the solicitude that they show large corporate accounts¹² and on other occasions attacking them as they would any other competitor. Resale carrier customers, however, are not like other rival providers; they are entirely dependent on their network service providers for service and hence are extremely vulnerable to anticompetitive abuses perpetrated by such entities. Of direct consequence here, a resale carrier's network service provider can inflict severe damage on the resale carrier's business by abusing competitively-sensitive information received from the resale carrier. Obviously, significant erosion of a resale carrier's customer base through such conduct can have devastating, if not fatal, consequences.

cert. granted sub. nom AT&T Corp. v. Iowa Utilities Board (Nov. 17, 1997), *pet. for rev. pending sub. nom., Southwestern Bell Telephone Co. v. FCC*, Case No. 97-3389 (Sept. 5, 1997).

¹¹ As the Commission has recognized, "small businesses are able to serve narrower niche markets that may not be easily or profitably served by large corporations, especially as large telecommunications expand globally." Section 257 Proceeding to Identify and Eliminate Market Entry Barriers for Small Businesses (Notice of Inquiry), GN Docket No. 96-113, ¶ 6 (1996).

¹² Competition in the Interstate, Interexchange Marketplace, 6 FCC Rcd. 5880 at ¶ 115 (resale customers as "valued customers").

As noted above, resale carriers in the past were left to argue that appropriation by network service providers of confidential data disclosed to them by resale carrier customers constituted an abuse of common law common carrier obligations. There was no express prohibition barring a network service provider from using information about a resale carrier customer's subscribers obtained through the customer/carrier relationship with the resale carrier to market its services to those subscribers. The customer proprietary network information ("CPNI") safeguards established by the Commission in its *Computer II* and *Computer III Decisions* were designed primarily to protect the privacy of end user customers and to safeguard rival enhanced service providers ("ESPs") and competing suppliers of customer premises equipment ("CPE") from discrimination by AT&T, the Bell Operating Companies ("BOCs") and GTE Corporation ("GTE").¹³ These safeguards limited the ability of carriers to use CPNI obtained through provision of regulated services to their own customers in order to gain an anticompetitive advantage in the unregulated CPE and enhanced services market.

¹³ See, e.g., Amendment of Sections 64.702 of the Commission's Rules and Regulations (Second Computer Inquiry), 77 F.C.C.2d 384 (1980), *recon.* 84 F.C.C.2d 50 (1980), *further recon.* 88 F.C.C.2d 512 (1981), *aff'd sub nom. Computer and Communications Industry Association v. FCC*, 693 F.2d 198 (D.C.Cir. 1984), *cert denied sub nom. Louisiana Public Service Commission v. FCC*, 461 U.S. 938 (1983), *further recon.* FCC 84-190 (released May 4, 1984); Amendment of Sections 64.702 of the Commission's Rules and Regulations (Third Computer Inquiry), Phase I: 104 F.C.C. 2d 958 (1956), *recon.* 2 FCC Rcd. 3035 (1987), *further recon.* 3 FCC Rcd. 1135 (1988), *further recon.* 4 FCC Rcd. 5927 (1989), *rev'd sub nom. California v. FCC*, 905 F.2d 1217 (9th Cir. 1990); Phase II: 2 FCC Rcd. 3072 (1987), *further recon.* 3 FCC Rcd. 1150 (1988), *further recon.* 4 FCC Rcd. 5927 (1989), *rev'd sub nom. California v. FCC*, 905 F.2d 1217 (9th Cir. 1990); Computer III Remand Proceedings, 5 FCC Rcd. 7719 (1990), *recon.* 7 FCC Rcd. 909 (1992), *aff'd sub nom. California v. FCC*, 4 F.3d 1505 (9th Cir. 1993); Computer III Remand Proceedings: Bell Operating Company Safeguards and Tier I Local Exchange Company Safeguards, 6 FCC Rcd. 7571 (1991), *recon.* 11 FCC Rcd. 12513 (1996), *rev'd in part sub nom. California v. FCC*, 39 F.3d 919 (9th Cir. 1994), *cert. denied* 115 S.Ct. 1427 (1995).

Applying these rules to abuses by a network service provider of its resale carrier customers' confidential data was akin to forcing a square peg into a round hole. The network service provider and the resale carrier customer were engaged in providing the same regulated services. Moreover, the "customer" whose information was being misused was the resale carrier, not the end user; indeed, the network service provider had no relationship whatsoever with the end user. And the overriding concern was not preventing the regulated side of the carrier operation from sharing information with the unregulated side, rather the focus was on preventing such information sharing within the regulated operation between operational and retail marketing personnel.

The Telecommunications Act has changed all of this, adopting explicit safeguards for the competitively-sensitive data resale carriers must disclose to their network providers. Half the battle has thus been won. The remaining portion of the fight, however, is no less important. A statutory prohibition is meaningless unless it is enforceable and enforced. TRA urges the Commission to take this opportunity to put "teeth" into Sections 222(a) and 222(b), thereby realizing the Congressional intent that network providers should not be allowed to exploit their carrier/customer relationship with their resale carrier customers by abusing confidential data disclosed in furtherance of that relationship to appropriate the resale carrier customer's subscribers. As the Congress made clear in the Telecommunications Act, competition should be fair and equitable; no competitor should be afforded an anticompetitive advantage.

II.

RECOMMENDATIONS

As noted above, new Sections 222(a) and 222(b) of the Communications Act contain the express safeguards long sought by resale carriers against abuse of the competitively-sensitive data they must disclose to network providers in order to obtain network services. Section 222(a) imposes on all telecommunications carriers, including interexchange carriers ("IXCs"), incumbent LECs, competitive access providers ("CAPs"), competitive LECs, cellular, personal communications services ("PCS") and other wireless providers and, for that matter, wholesale resale carriers, the duty to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, including telecommunications carriers reselling their services.¹⁴ Section 222(b) enhances this obligation by prohibiting the use by a telecommunications carrier in its own marketing efforts of proprietary information it receives or obtains from another carrier for purposes of providing a telecommunications service; indeed, Section 222(b) mandates that such proprietary information may be used only for the purpose of providing telecommunications service to that other carrier.¹⁵ In other words, Sections 222(a) and 222(b) together bar a network service provider from using for its own benefit the confidential information disclosed to it by a resale carrier customer, essentially reaffirming and codifying the age old common law common carrier obligation.

The duties and obligations set forth in new Sections 222(a) and 222(b) of the Communications Act are remarkably clear and direct. Little, if any, "interpretation" of Sections

¹⁴ 47 U.S.C. § 222(a).

¹⁵ 47 U.S.C. § 222(b).

222(a) and 222(b) is thus required. If, however, Sections 222(a) and 222(b) are to have their intended effect, promulgation of implementing regulations is nonetheless essential.

The Commission's principal objective in adopting implementing regulations should be to ensure that a network service provider's retail sales and marketing personnel are not privy to, and do not have access to databases containing, information regarding the subscribers of the network service provider's resale carrier customers. Achieving this goal will require not only effective access restrictions, but incentives significant enough to motivate strict carrier compliance. Three steps are necessary to accomplish these twin ends. First, the Commission must require network service providers to "wall-off" resale carrier confidential data from retail sales and marketing personnel. Second, the Commission must hold network service providers to a strict liability standard for abuse of resale carrier confidential data by their employees or agents. And third, the Commission must rigorously enforce the mandates of Sections 222(a) and 222(b) by imposing heavy monetary sanctions for abuse of resale carrier confidential data.

Access restrictions are the only means that may be effective in insulating resale carrier confidential data from network service provider retail sales and marketing personnel. Marketing and sales personnel obviously have strong incentives to increase sales and subscriber counts. Whether direct -- *e.g.*, commission compensation arrangements -- or indirect -- *e.g.*, salary increases or position advancement --, these incentives often drive individuals to bend or break rules, particularly if they know that the penalties for such conduct are likely not to be severe. Human nature being what it is, marketing and sales personnel seek advantages wherever they can be found, and the subscriber lists of resale carrier customers, particularly when supplemented by detailed data revealing such critical information as service requirements, traffic levels and usage data, provide

highly attractive leads. Thus while personnel training and corporate certifications may well be useful adjuncts to access restrictions, neither personnel training nor corporate certifications nor, for that matter, use restrictions or access documentation will likely be effective in preventing abuse of resale carrier confidential data.

During the period when 90 percent of those resale carriers using AT&T as their network service provider reported that AT&T was using their carrier confidential data to solicit their customers and more than 85 percent and 60 percent, respectively, of these AT&T resellers characterized the abuse of carrier confidential data as serious or very serious and the occurrences of such abuse as frequent or very frequent, AT&T purportedly had in place multiple safeguards against such abuses. Company policies decrying abuse of resale carrier confidential data had been announced, databases were apparently monitored, and "rogue" employees were said to be subject to sanctions. And AT&T repeatedly assured the Commission during this period that the controls it had in place were adequate.¹⁶ The problems nonetheless persisted and they did so because the databases containing resale carrier confidential data were accessible by AT&T retail sales and marketing personnel.

TRA is aware that the Commission declined to require access restrictions which would have "prohibit[ed] carrier personnel from accessing CPNI of customers who have either failed, or expressly declined, to give requisite approval for carrier use of CPNI for marketing

¹⁶ See, e.g., Letter from Judy Arenstein, Government Affairs Vice President, AT&T Corp., to William F. Caton, Acting Secretary, Federal Communications Commission, dated August 14, 1995, filed in CC Docket No. 79-252 ("What is AT&T doing to protect ['proprietary business information AT&T has solely because the reseller is our customer']? Continuously enhances security system; Repeatedly reinforces CPNI policy; Investigates specific allegations of CPNI abuse").

purposes."¹⁷ Many of the reasons given for this action, however, do not apply to restricting access by retail sales and marketing personnel to resale carrier confidential data. For example, the Commission "conclude[d] that general access restrictions are not compatible with the exception set forth in section 222(d)(3), which expressly permits carriers to use CPNI for marketing purposes when customers so approve during inbound calls."¹⁸ Unlike end-user CPNI, there will never be an instance in which a network service provider's retail sales and marketing personnel will have a legitimate need to access resale carrier confidential data.

While the Commission was not persuaded that "the increased protection afforded through access restrictions or separate marketing personnel would justify the additional expense of [a mechanical access system]," opining that "use restrictions . . . can and will be effective when coupled with personnel training,"¹⁹ the experience of TRA and its resale carrier members simply does not bear out this optimistic assessment. As noted above, use restrictions and personnel training have not in the past proven adequate to protect the confidential data of resale carriers. Moreover, TRA finds it inconceivable that the mere introduction of database restrictions which bar access by retail sales and marketing personnel to resale carrier confidential data could cost, as suggested by U S WEST, upwards to \$100 million.²⁰ More inconceivable to TRA is the notion that databases containing resale carrier confidential data are not already access restricted to some degree -- *e.g.* to outside parties. And TRA strenuously disagrees that the highest potential for "dampen[ing]

¹⁷ Notice, FCC 98-27 at ¶ 195.

¹⁸ Id.

¹⁹ Id. at ¶ 197.

²⁰ Id. at ¶ 197, fn 687.

competition" from "small carriers" is the cost of access restrictions on resale carrier confidential data;²¹ rather, the compelling threat to small carriers competing with the retail operations of their generally far larger network service providers is access by the network service provider's retail sales and marketing personnel to resale carrier confidential data.

In short, if the will of Congress that network service providers should not be permitted to exploit for their own marketing advantage the confidential data secured from resale carrier customers solely by virtue of their provision of wholesale services to these resale carriers is to have meaning, the network service providers' retail sales and marketing personnel must be denied physical and logical access to resale carrier confidential data. Anything short of access restrictions will expose resale carriers to the very conduct that caused them to lobby so hard for the protections embodied in Sections 222(a) and 222(b).

Also of critical importance, the Commission must hold network service providers strictly accountable for abuses of resale carrier confidential data perpetrated by their employees and agents. It is after all, the network service provider that will have constructed and will control, as well as police, the internal safeguards and procedures that will have proven to be inadequate in the event of abuse of resale carrier confidential data. It is the network service provider that will have determined the adequacy of these safeguards and procedures, realizing the benefits of any cost or administrative savings from use of lesser measures. And it is of course the network service provider that will realize the benefits from the illicit marketing successes of their retail sales and marketing

²¹ Id. at ¶ 197.

personnel. TRA submits that it is, therefore, the network service provider that should bear the liability burden for any failure of its systems.

Resale carriers have no say in the internal database controls or personnel policies of their network providers, yet in the absence of a strict liability standard, it is the resale carriers that would bear the brunt of abuses of their carrier confidential data by the retail sales and marketing personnel of their network service providers. Equity demands that the entity in the best position to prevent an unlawful act should bear the responsibility for commission of that act, particularly if the same entity stands to benefit from that act.

Of course, a strict liability standard is meaningless unless it is accompanied by heavy monetary penalties. It belabors the obvious to suggest that it is extremely difficult to document abuses of resale carrier confidential data by network service providers. Each documented violation generally represents many more undocumentable violations. Network service providers benefit directly from each such violation; conversely, resale carriers are harmed by each such violation. Unless there is a legitimate fear of sanctions, there will be little, if any, disincentive for conduct contrary to the dictates of Sections 222(a) and 222(b), particularly given that few, if any, violations will actually be uncovered and if discovered will be adequately documented. TRA, accordingly, submits that when abuses are proven, sanctions must be applied expeditiously and far outweigh the benefit derived from the unlawful conduct. Moreover, corporate officers that attest to their company's compliance with Section 222(b)'s prohibition against use of resale carrier confidential data should be held personally accountable for any false certifications.

As TRA has stressed above, customer bases are the principal, if not the exclusive, asset of resale carriers. Appropriation of resale carrier confidential data to raid resale carriers'

customer bases is theft pure and simple. The protections embodied in Sections 222(a) and 222(b) have been a long time coming and the product of much work by the resale carrier community. TRA urges the Commission in the strongest possible terms not to negate these critical safeguards by adopting inadequate implementing regulations. Access restrictions, accompanied by strict liability and serious penalties, are necessary to fulfill a clear Congressional mandate.

III.

CONCLUSION

By reason of the foregoing, the Telecommunications Resellers Association urges the Commission to adopt rules and policies in this docket consistent with these comments.

Respectfully submitted,

TELECOMMUNICATIONS RESELLERS ASSOCIATION

By: 

Charles C. Hunter
Catherine M. Hannan
HUNTER COMMUNICATIONS LAW GROUP
1620 I Street, N.W.
Suite 701
Washington, D.C. 20006
(202) 293-2500

March 30, 1998

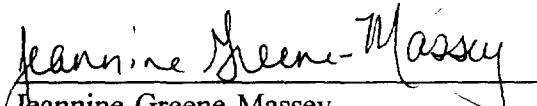
Its Attorneys

CERTIFICATE OF SERVICE

I, Jeannine Greene-Massey, hereby certify that copies of the foregoing document were hand delivered this 30th day of March, 1998, to the following:

Ms. Janice Myles
Federal Communications Commission
Common Carrier Bureau
1919 M Street, N.W.
Room 544
Washington, DC 20554

International Transcription Services, Inc.
1231 20th Street, N.W.
Washington, DC 20036


Jeannine Greene-Massey